UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,142	04/15/2004	Deanna Lynn Quigg Brown	AUS920040197US1	7822

35525 7590 10/21/2008

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
TORRES, JOSEPH D	
ART UNIT	PAPER NUMBER
2112	

NOTIFICATION DATE	DELIVERY MODE
10/21/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptonotifs@yeeiplaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/825,142	BROWN ET AL.	
	Examiner	Art Unit	
	Joseph D. Torres	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-39* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claim 28 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. While features of an apparatus may be recited either structurally or functionally, claims directed to an apparatus must be distinguished from the prior art in terms of structure rather than function, because apparatus claims cover what a device is, not what a device does (Hewlett-Packard Co. v. Bausch & Lomb Inc., 909 F.2d 1464, 1469, 15 USPQ2d 1525, 1528 (Fed. Cir. 1990)).

The language in claim 28 is descriptive in nature describing the structure of an abstract packet data structure. Claim 28 fails to recite any structural element that further limits the apparatus of claim 15.

As per claim 28: claim 28 does not recite any limitation that can be regarded as a structural element or structural interconnection further limiting the apparatus of claim 15, claim 14 instead recites attributes of a data structure.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. While features of an apparatus may be recited either structurally or functionally, claims directed to an apparatus must be distinguished from the prior art in terms of structure rather than function, because apparatus claims cover what a device is, not what a device does (Hewlett-Packard Co. v. Bausch & Lomb Inc., 909 F.2d 1464, 1469, 15 USPQ2d 1525, 1528 (Fed. Cir. 1990)). The omitted structural cooperative relationships are: any structural elements connecting the data structures in claim 28 to the steps of claim 15.

As per claim 28: claim 28 does not recite any limitation that can be regarded as a structural element or structural interconnection further limiting the apparatus of claim 15, claim 14 instead recites attributes of a data structure.

Claim Rejections - 35 USC § 101

The Applicant contends, "The Examiner notes terminology in the present Specification at page 30 that can be interpreted to mean that recordable-type media includes transmission-type media. Applicants urge that such transmission-type media description was previously removed from the Specification (Response to Office Action filed on February 6, 2008), and thus the Examiner's quotation of "recordable-type media" being defined in the Specification as encompassing "transmission-type media" is erroneous, as the Specification defines recordable-type media to b media such as

floppy disk, a hard disk drive, a RAM, CD-ROMs, and DVD-ROMs. Importantly, Claim 29 is directed to recordable-type media, and is not directed transmission-type media.".

Since the Appl9icant has placed an Estoppel on the interpretation of recordable-type media as "transmission-type media" and furthermore has restricted the definition to commonly known recordable devices such as floppy disk, a hard disk drive, a RAM, CD-ROMs, DVD-ROMs; the Examiner withdraws the prior 101 rejections.

Response to Arguments

Applicant's arguments filed 08/14/2008 have been fully considered but they are not persuasive.

The Applicant contends, "With respect to Claim 28, the Examiner states that such claim does not recite any limitation that can be regarded as a structural element or structural interconnection further limiting the method of Claim 1. Applicants urge that Claim 28 depends upon system Claim 15, and therefore does not need to further limit Claim 1. In addition, Claim 28 recites a structural element (the particular structural location of the flags)".

The Examiner asserts that anyone serious about advancing prosecution would have recognized from context that claim 1 is a typo and would have made appropriate corrections.

The Applicant contends, "The Examiner notes terminology in the present Specification at page 30 that can be interpreted to mean that recordable-type media includes transmission-type media. Applicants urge that such transmission-type media description was previously removed from the Specification (Response to Office Action filed on February 6, 2008), and thus the Examiner's quotation of "recordable-type media" being defined in the Specification as encompassing "transmission-type media" is erroneous, as the Specification defines recordable-type media to b media such as floppy disk, a hard disk drive, a RAM, CD-ROMs, and DVD-ROMs. Importantly, Claim 29 is directed to recordable-type media, and is not directed transmission-type media.".

Since the Applicant has placed an Estoppel on the interpretation of recordable-type media as "transmission-type media" and furthermore has restricted the definition to commonly known recordable devices such as floppy disk, a hard disk drive, a RAM, CD-ROMs, DVD-ROMs; the Examiner withdraws the prior 101 rejections.

The Applicant contends, "The cited passage at Thompson col. 8, however, describes various operational steps that are performed when a data packet is to be *transmitted*. The receipt and transmission of data packets are separate and distinct operations, and steps describing operational steps with respect to *transmission* of data packets, such as those described by Thompson at col. 8, do not provide any description or teaching with respect to operational steps that occur upon *receiving* a data packet, which is what Claim 1 is directed to. Thus, Thompson's description at col. 8 does not provide any teaching as to any operational steps that occur "responsive to receiving" a data packet,

as is recited in Claim 1. Thus, the Examiner's reliance on Thompson's teachings at col. 8 - which is directed to steps that occur in anticipation of a data packet being *transmitted* - does not provide any teaching/description of any operational steps that occur responsive to *receiving* the data packet, as per the features of Claim 1.".

The Examiner disagrees and asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

The Applicant contends, "Thompson's teachings at col. 3 with respect to checksum processing occurs unconditionally, and such checksum processing is not described as being performed 'as indicated by the state of the first flag and the state of the second flag', as per the features of Claim 1. Instead, this cited passage states that the packet header is 'decoded', a checksum is 'calculated', which is then 'compared' with the received checksum in the received data packet. There is *no selective verification of the checksum of a received data packet as indicated by the state of* ***two flags that are received***, as per the features expressly recited in Claim 1".

The Examiner disagrees and asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a

receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

Furthermore, if a packet does not have a checksum it is impossible to perform checksumming on the packet; hence the Applicant's notion that unconditional checksumming without regard to critical information on he checksum provided by flag fields for the checksum is absurd.

The Applicant contends, "Further with respect to Thompson's description at col. 8 regarding outbound packet data processing, to the extent such passage describes flags, these flags do not indicate whether to selectively verify a checksum in a received data packet, but instead indicate whether a checksum is to be inserted in an outbound packet. This is different from Claim 1 in that 'insertion' of a checksum is substantially different from 'verifying' a checksum, and processing associated with an 'outbound' packet has nothing to do with processing of an inbound/received data packet, as per the features of Claim 1. Nor are these flags described as being part of a data packet that is received, as per the features of Claim 1. Thus, it is further shown that Claim 1 has been erroneously rejected as Thompson's flags are not used to indicate selective verification of a received data packet, but instead indicates whether a checksum is to be inserted in an outbound data packet."

The Examiner disagrees and asserts col. 8 in Thompson explicitly teaches header control information that is added to an oubound packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the

packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is added to an outbound packet to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

The Applicant contention that "Thompson's flags are not used to indicate selective verification of a received data packet, but instead indicates whether a checksum is to be inserted in an outbound data packet" again is absurd for, if such were the case, there would be no reason to include the checksum information in the outbound packet. That is, the sole reason for including the checksum information in the outbound packet is to inform a receiving node about availability of checksumming and, if checksumming is available, "the byte at which checksumming is to start", "the number of bytes which are

to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)".

The Applicant contends, "With respect to Claim 1, such claim recites "selectively verifying a checksum, by the first partition in the logical partitioned data processing system, for the data packet as indicated by the state of the first flag and the state of the second flag, wherein the first flag and the second flag are both checksum- based flags that indicate checksum characteristics associated with the data packet". As can be seen, such claimed features are directed to a conditional CRC check based on two different flags. In reaching the conclusion that all three references (Kondo, Maezawa and implicitly in Lansing) describe a CRC check being based on a CRC flag (which Applicants deny, as will be further shown below), the Examiner mischaracterizes the teachings of the cited reference. For example, on page 10 of the present Office Action dated July 3, 2008, the Examiner states: "the flag in Kondo providing an indication of whether redundancy exists" Applicants urge clear error in such assertion, as the Kondo flag does not provide any indication of whether redundancy exists - instead the Kondo flag provides an indication of whether an ECC error exists. An ECC error indicator does not provide any information as to whether redundancy exists, but instead provides an indication of whether an error exists. This can be seen by Kondo' s description at col. 39, lines 62-65, where it states: "When checking the CIP header 2701, the ECC flag 2702 contained therein is examined. When the ECC flag indicates "no ECC error", CRC check on the AV data 2704 is performed." Thus, contrary to the Examiner's assertion,

Kondo's flag does not provide any indication of whether redundancy exists, but instead provides an indication of whether an error exists. As this Kondo mischaracterization is used in establishing why the claims are obvious in view of the cited references, it is urged that such obviousness conclusion is flawed as relying upon such improper characterization of what Kondo actually describes".

The Examiner suggests that the Applicant reread the rejection filed July 3, 2008 in which the Examiner provides the following observations: "Kondo and Lansing, in an analogous art, teaches use of identifying a state of a first flag (Step 905 in Figure 9 and claim 1 in Lansing teaches identifying a state of a first CRC flag used to indicate the presence of redundancy) and a state of a second flag (col. 39, lines 55-67 in Kondo teaches a second ECC flag in a packet indicating whether error are present in the packet or not) in the data packet; and selectively verifying a checksum based on the state of the first flag (Steps 905-915 in Figure 9 of Lansing) and the state of the second flag (col. 39, lines 62-67 in Kondo teaches identifying/detecting the second ECC flag to selectively verify the CRC checksum)."

The Examiner asserts that anyone serious about advancing prosecution would have recognized from context of the rejection that ""the flag in Kondo providing an indication of whether redundancy exists"" is a typo and furthermore it is clear that the combined teaching of Kondo and Lansing provide two different flags used in check sum verification.

The Applicant contends, “Further with respect to Claim 1, the cited Maezawa reference describes, as expressly acknowledged by the Examiner, that each packet has a CRC checksum used for verifying received data (see page 9 of the present Office Action dated July 3, 2008, lines 6-9), and thus it is urged that a person of ordinary skill in the art would not have been motivated to modify such Maezawa teachings of verifying each packet in accordance with the claimed feature of 'selectively verifying' due to this Maezawa desire to verify each packet. Thus, the only motivation for making such a change must be coming from Applicants' own disclosure and claims, which is impermissible hindsight analysis”.

The Examiner disagrees and asserts both Thompson, Kondo and Lansing provide motivation for providing the particular motivation for using flags in the Kondo and Lansing patents: because one of ordinary skill in the art would have recognized that use of identifying a state of a first flag and a state of a second flag in the data packet; and selectively verifying a checksum based on the state of the first flag and the state of the second flag would have provided a flexible arrangement whereby the packet creator can decide whether CRC is needed (Abstract in Lansing) and would have provided flagging for erroneous data for use by system controllers (col. 35, lines 55-62 in Kondo) and ould havew provided control information for checksumming (Abstract in Thompson). Furthermore; it could be said that the Applicant is the one who gleaned insight from the Kondo and Lansing patents.

The Applicant contends, “Applicants urge that the Maezawa description does not describe the claimed 'interpartition virtual network' since such reference does not describe "wherein each one of the logical partitions comprises a virtual network adapter that is used to send data packets to other virtual network adapters of other logical partitions within the logical partitioned data processing system to thereby form the interpartition virtual network". As Claim 1 explicitly defines the claimed 'interpartition virtual network' to be a network where each one of the logical partitions comprises a virtual network adapter that is used to send data packets to other virtual network adapters of other logical partitions within the logical partitioned data processing system, and the cited Maezawa reference does not describe such virtual network adapters or their associated claimed features, Maezawa cannot describe or teach the claimed interpartition virtual network. Accordingly, as Maezawa cannot describe/teach the claimed interpartition virtual network, it necessarily logically follows that Maezawa also cannot describe/teach data packet transfer in such a (missing) interpartition virtual network. Thus, contrary to the Examiner's assertion in rejecting Claim 1, Maezawa does not teach the claimed interpartition virtual network, or the receiving of a data packet at a first partition of such (missing) interpartition virtual network. Thus, it is further urged that Claim 1 has been erroneously rejected due to this additional prima facie obviousness deficiency”.

The Examiner disagrees and asserts col. 3, lines 60-65, col. 12, lines 1-12 and Figure 1 in Maezawa clearly suggest receiving data packets at a first partition in the interpartition virtual network of Figure 3 from a second partition in the interpartition virtual network of

Figure 3 in the logical partitioned data processing system of Figure 3. The Examiner asserts that the Applicant's arguments are illogical in that one of ordinary skill in the art at the time the invention was made would have to go to extraordinary lengths to avoid interpartition packet communications in a system that is designed for interpartition packet communications such as the one in Figure 3 of Maezawa.

The Applicant contends, "As to the cited Thompson passage at col. 3, which is directed to steps that occur when receiving a data packet, this description describes a traditional checksum calculation being unconditionally performed by the network adapter, including steps of decoding, programming, calculating, transferring, appending and comparing. Such traditional checksum calculation has already been expressly acknowledged by Applicants in the background section of their own Specification (page 1, lines 12-27; "Description of Related Art"). As to the cited Thompson passage at Col. 3, which is directed to steps that occur when receiving a data packet, this description describes a traditional checksum calculation being unconditionally performed by the network adapter, including steps of decoding, programming, calculating, transferring, appending and comparing. Such traditional checksum calculation has already been expressly acknowledged by Applicants in the background section of their own Specification (page 1, lines 12-27; "Description of Related Art"). The operational steps with respect to transmission of data packets, such as those described by Thompson at the cited col. 8 passage, do not provide any description or teaching with respect to operational steps

that occur upon receiving a data packet, which is what Claim 1 is directed to. Quite simply, Thompson's description at col. 8 does not provide any teaching as to any".

The Examiner disagrees and asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

Furthermore, if a packet does not have a checksum it is impossible to perform checksumming on the packet; hence the Applicant's notion that traditional checksumming without regard to critical information on the checksum provided by flag fields for the checksum is absurd.

The Applicant contends, “none of me cited references teach or suggest the claimed feature of "wherein the first flag is a no checksum flag that is used by the selectively verifying step to determine whether or not there is a checksum value included in the data packet that is received and the second flag is a checksum good flag that is used by the selectively verifying step to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received". As can be seen, the features of Claim 2 are directed to features/characteristics associated with the two flags. Specifically, the first flag is a no checksum flag that is used by the selectively verifying step to determine whether or not there is a checksum value included in the data packet that is received. The second flag is a checksum good flag that is used by the selectively verifying step to determine whether or not the data packet has previously been verified as being good based on a checksum included in the data packet that is received. In rejecting Claim 2, the Examiner cites Kondo col. 39, lines 55-67 and Lansing' s step 905 of Figure 9 as teachings the features of Claim 2. Applicants urge clear error in such assertion, as will now be described in detail. Kondo describes at col. 39, line 55-67 an ECC flag that indicates whether or not there is an ECC error. Such ECC flag (1) is not used by a selectively verifying step to determine whether or not there is a checksum value included in the data packet that is received (and thus this ECC flag is not equivalent to the claimed first flag) - instead this flag indicates if there is an error, and (2) is not used by a selectively verifying step to determine whether or not the data packet has

previously been verified as being good based on a checksum included in the data packet that is received (and thus this ECC flag is not equivalent to the claimed second flag) - instead this ECC flag indicates if there is an error.".

The Examiner disagrees and asserts that a ECC flag indicates if there is an error when it is set is also an ECC flag that indicates that there is no error when the flag is not set, hence; an ECC flag indicates if there is an error is also a checksum good flag since it can indicate no errors when the flag is not set.

The Applicant contends, "Further with respect to Claim 4, such claim recites "wherein the selectively verifying step includes: skipping verification of the checksum if the first flag is set". As can be seen, the features of Claim 4 are directed to particulars associated with the selectively verifying step, where checksum verification is skipped if the first flag is set. The Examiner asserts that Lansing teaches such selectively verifying details at Figure 9, elements 905-915. Applicants urge clear error, as this cited Lansing passage: (1) is not directed to any type of verification step, but instead is directed to a generation step (Lansing Figure 9, element 910), and (2) does not describe any skipping of checksum verification, but instead is directed to skipping a checksum generation step (Lansing Figure 9, element 910). Thus, contrary to the Examiner's assertion, Lansing does not teach the features expressly recited in Claim 4, and therefore it is further urged that Claim 4 has been erroneously rejected due to this additional prima facie obviousness deficiency".

The Examiner disagrees and asserts that if a packet does not have a checksum it is impossible to perform checksumming on the packet. The intent in Lansing is clear.

The Applicant contends, “Further with respect to Claim 6, such claim recites "wherein the second flag is conditionally unset by the logical partitioned data processing system if the packet was received through a first virtual adapter associated with the first partition". As can be seen, the features of Claim 6 are specifically directed to a conditional unsetting of the second flag, where such condition is "if the packet was received through a first virtual adapter associated with the first partition". The Examiner makes no assertion as to any teaching with respect to the condition regarding how that packet was received”.

The Examiner disagrees and asserts that the flags in Kondo, Lansing and Thompson are adaptively provided at each receiving and transmitting node and are adaptively set or unset at each node as packets are transferred across a communication system.

The Applicant contends, “Further with respect to Claim 8 (and dependent Claims 9 and 10), such claim recites "wherein the second flag is conditionally unset by the logical partitioned data processing system if the data packet, received from the second partition, was received from outside the interpartition virtual network in the logical partitioned data processing system without the checksum being checked". As can be seen, the features of Claim 8 are specifically directed to conditionally unsetting the second flag, where such condition is "if the data packet, received from the second

partition, was received from outside the interpartition virtual network in the logical partitioned data processing system without the checksum being checked". The Examiner makes no assertion as to any teaching with respect to the condition regarding how that packet was received”.

The Examiner disagrees and asserts that the flags in Kondo, Lansing and Thompson are adaptively provided at each receiving and transmitting node and are adaptively set or unset at each node as packets are transferred across a communication system.

The Applicant contends, “Further with respect to Claim 9, such claim recites "wherein the first flag is conditionally unset by the logical partitioned data processing system and the second flag is conditionally unset by the logical partitioned data processing system if the data packet was received by a physical network adapter that (i) is associated with the second partition, and (ii) does not support checksum offload". As can be seen, the features of Claim 9 are specifically directed to a conditional unsetting of the first and second flags, where such condition is "if the data packet was received by a physical network adapter that (i) is associated with the second partition, and (ii) does not support checksum offioad". The Examiner makes no assertion as to any teaching with respect to the condition regarding where the data packet originated”.

The Examiner disagrees and asserts that the flags in Kondo, Lansing and Thompson are adaptively provided at each receiving and transmitting node and are adaptively set or unset at each node as packets are transferred across a communication system.

The Applicant contends, “Further with respect to Claim 10, such claim recites "wherein the first flag is conditionally unset by the logical partitioned data processing system and the second flag is conditionally set by the logical partitioned data processing system if a physical adapter, supporting a checksum offioad, verified the checksum as being good". As can be seen, the features of Claim 10 are specifically directed to a conditional unsetting of the first flag and conditional setting of the second flag, where such condition is "if a physical adapter, supporting a checksum offload, verified the checksum as being good". The Examiner makes no assertion as to any teaching with respect to the condition regarding where the data packet originated”.

The Examiner disagrees and asserts that the flags in Kondo, Lansing and Thompson are adaptively provided at each receiving and transmitting node and are adaptively set or unset at each node as packets are transferred across a communication system.

The Applicant contends, “With respect to Claim 11, such claim recites "wherein the first virtual adapter is a software device driver that has no associated physical hardware". In rejecting Claim 11, the Examiner states that Maezawa teaches the features of Claim 11 by Maezawa's multiplexor channel devices 3 and 10 in Figure 1. Applicants urge that such physical hardware devices do not teach "wherein the first virtual adapter is a software device driver that has no associated physical hardware", as per the features of Claim 11. Therefore, it is further urged that Claim 11 has been erroneously rejected due to this additional prima facie obviousness deficiency”.

The Examiner disagrees and asserts Claims 1-14 are a method for processing data.

"wherein the first virtual adapter is a software device driver that has no associated physical hardware" is a statement of intended use for the method and fails to set forth a positive limitation for a method for processing data.

The Applicant contends, “Further with respect to Claim 13, such claim recites "wherein the first flag and the second flag are added to a header of the data packet that is received by firmware of the logical data processing system during routing of the data packet, to a given partition of the logical partitioned data processing system, by the firmware". As can be seen, the features of Claim 13 are specifically directed to a particular technique for adding flags to a header of a data packet. In rejecting Claim 13, the Examiner states that Maezawa teaches a means for sending by Maezawa's circuits 37 and 38 of Figure 2. Applicants urge clear error, as Claim 13 was previously amended to recited data packet header operations in combination with firmware, and does not recite any type of means for sending, as alleged by the Examiner. Therefore, it is further urged that Claim 13 has been erroneously rejected due to this additional prima facie obviousness deficiency.”

The Examiner disagrees and asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach “Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76” to selectively indicate to a receiver “the byte at which checksumming is to

start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1, 15, 29 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson; Michael I. et al. (US 5430842 A, hereafter referred to as Thompson) in view of Hefferon; Eugene Paul et al. (US 5659756 A, hereafter referred to as Hefferon) and Bean; George H. et al. (US 4843541 A, hereafter referred to as Bean).

35 U.S.C. 103(a) rejection of claims 1, 15, 29 and 39.

Thompson teaches responsive to receiving the data packet at a first partition of a data processing system from a second partition of a data processing system, identifying a state of a first flag and a state of a second flag in the data packet (Col. 3, lines 40-49 and col. 8, lines 13-27 of Thompson teaches checksum control information including first flag 74 and second flag 72, responsive to receiving the data packet at a first partition 22 in Figure 2 of Thompson of a data processing system from a second partition 12 in Figure 2 of Thompson of a data processing system, is used for identifying a state of first flag 74 and a state of second flag 72 in the data packet in order to verify datqa); and selectively verifying a checksum, by the first partition in the logical partitioned data processing system, for the data packet as indicated by the state of the first flag and the state of the second flag (Col. 3, lines 40-49 and col. 8, lines 13-27 of Thompson), wherein the first flag and the second flag are both checksum-based flags that indicate checksum characteristics associated with the data packet (col. 8, lines 13-27 of Thompson).

<u>The Examiner asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to</u>

inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

Furthermore, if a packet does not have a checksum it is impossible to perform checksumming on the packet; hence the Applicant's notion that unconditional checksumming without regard to critical information on he checksum provided by flag fields for the checksum is absurd.

In addition, there would be no reason to include the checksum information in the outbound packet, if it were not used by a receiving node. That is, the sole reason

for including the checksum information in the outbound packet is to inform a receiving node about availability of checksumming and, if checksumming is available, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)".

However Thompson does not explicitly teach the specific use of a logical partitioned data processing system.

Hefferon, in an analogous art, teaches use of a logical partitioned data processing system (Abstract in Hefferon).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hefferon with the teachings of Hefferon and Bean by including use of a logical partitioned data processing system. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that use of a logical partitioned data processing system would have provided highly efficient operation of a plurality of different programming systems in the different zones of the system (col. 1, lines 9-13 in Bean).

Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maezawa; Hirofumi et al. (US 6145024 A, hereafter referred to as Maezawa) in view of Kondo; Satoshi et al. (US 6618396 B1, hereafter referred to as Kondo) and Lansing, Shane P. et al. (US 20030058862 A1, hereafter referred to as Lansing) in further view of

Thompson; Michael I. et al. (US 5430842 A, hereafter referred to as Thompson) in view of Hefferon; Eugene Paul et al. (US 5659756 A, hereafter referred to as Hefferon) and Bean; George H. et al. (US 4843541 A, hereafter referred to as Bean).

35 U.S.C. 103(a) rejection of claims 1, 15, 29 and 39.

Maezawa teaches receiving a data packet at a first partition in the interpartition virtual network from a second partition in the interpartition virtual network in the logical partitioned data processing system (col. 3, lines 60-65, col. 12, lines 1-12 and Figure 1 in Maezawa clearly suggest receiving data packets at a first partition in the interpartition virtual network of Figure 3 from a second partition in the interpartition virtual network of Figure 3 in the logical partitioned data processing system of Figure 3); and verifying a checksum in a first partition in the logical partitioned data processing system for the data packet (Figure 5 in Maezawa teaches that each packet has a CRC checksum used for verifying received data, which clearly suggests verifying a checksum in a receiving first partition in the logical partitioned data processing system for the data packet responsive to receiving the data packet).

Note: Figure 1 explicitly teaches inter-partition devices Host Computer 1 and memory Control unit 6 disposed to communicate directly to each other via high and medium capacity lines 20 and 21 to provide Host computer direct access to main memory for Host Computer 1. Figurer 1 in Maezawa also teaches a Switching device 7 for providing communication to other devices external to Host computer 1 and its own main memory. The internal direct connections between a host computer and its own main

memory is an inter-partition network. Col. 8, lines 41-50 make clear that the switching device 7 can be used to create virtual connections to any device on the network including main memory Control unit 6 for Host computer 1 to create an inter-partition virtual network. That is, the inter-partition virtual network comprising main memory Control unit 6 and Host computer 1 is disposed to communicate directly or virtually via switching device 7 in order to receive data packets at a first partition Host computer 1 in the interpartition virtual network of Figure 3 from a second partition memory Control unit 6 in the interpartition virtual network of Figure 3 in the logical partitioned data processing system of Figure 3.

The Examiner asserts col. 3, lines 60-65, col. 12, lines 1-12 and Figure 1 in Maezawa clearly suggest receiving data packets at a first partition in the interpartition virtual network of Figure 3 from a second partition in the interpartition virtual network of Figure 3 in the logical partitioned data processing system of Figure 3. The Examiner asserts that one of ordinary skill in the art at the time the invention was made would have to go to extraordinary lengths to avoid interpartition packet communications in a system that is designed for interpartition packet communications such as the one in Figure 3 of Maezawa. However Maezawa does not explicitly teach the specific use of **identifying a state of a first flag and a state of a second flag in the data packet**; and **selectively** verifying a checksum **based on the state of the first flag and the state of the second flag**. **Kondo and Lansing, in an analogous art, teaches use of identifying a state of a first flag (Step 905 in Figure 9 and claim 1 in Lansing teaches identifying a state**

of a first CRC flag used to indicate the presence of redundancy) and a state of a second flag (col. 39, lines 55-67 in Kondo teaches a second ECC flag in a packet indicating whether error are present in the packet or not) in the data packet; and selectively verifying a checksum based on the state of the first flag (Steps 905-915 in Figure 9 of Lansing) and the state of the second flag (col. 39, lines 62-67 in Kondo teaches identifying/detecting the second ECC flag to selectively verify the CRC checksum). Note: the flags in Kondo and Lansing are two distinct flags, the flag in Lansing providing an indication of whether redundancy exits (Note: it is well known that some protocols such as UDP do not require redundancy whereas TCP does; in a multi-protocol system such as the one in Maezawa this information is critical since checksum verification can only take place if redundancy exists) and the flag in Kondo indicates whether an error has been detected in a network device such as the switching device 7 in Maezawa used to forward data to an intended receiver). Col. 39, lines 62-67 in Kondo explicitly teaches performing a CRC check (i.e., checksum verification) responsive to the ECC flag. CRC generation is responsive to the CRC flag in Lansing and since the CRC check (i.e., checksum verification) in both Kondo and Maezawa (and implicitly in Lansing) is based on the presence of CRC, the CRC check (i.e., checksum verification) is also based on the CRC flag.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Maezawa with the teachings of Kondo and Lansing by including use of identifying a state of a first flag and a state of a second flag in the data

packet; and selectively verifying a checksum based on the state of the first flag and the state of the second flag. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that use of identifying a state of a first flag and a state of a second flag in the data packet; and selectively verifying a checksum based on the state of the first flag and the state of the second flag would have provided a flexible arrangement whereby the packet creator can decide whether CRC is needed (Abstract in Lansing) and would have provided flagging for erroneous data for use by system controllers (col. 35, lines 55-62 in Kondo).

Thompson teaches responsive to receiving the data packet at a first partition of a data processing system from a second partition of a data processing system, identifying a state of a first flag and a state of a second flag in the data packet (Col. 3, lines 40-49 and col. 8, lines 13-27 of Thompson teaches checksum control information including first flag 74 and second flag 72, responsive to receiving the data packet at a first partition 22 in Figure 2 of Thompson of a data processing system from a second partition 12 in Figure 2 of Thompson of a data processing system, is used for identifying a state of first flag 74 and a state of second flag 72 in the data packet in order to verify datqa); and selectively verifying a checksum, by the first partition in the logical partitioned data processing system, for the data packet as indicated by the state of the first flag and the state of the second flag (Col. 3, lines 40-49 and col. 8, lines 13-27 of Thompson), wherein the first flag and the second flag are both checksum-based flags

that indicate checksum characteristics associated with the data packet (col. 8, lines 13-27 of Thompson).

The Examiner asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

Furthermore, if a packet does not have a checksum it is impossible to perform checksumming on the packet; hence adaptive/selective checksumming with

regard to critical information on the checksum provided by flag fields for the checksum is required.

The Examiner asserts both Thompson, Kondo and Lansing provide motivation for providing the particular motivation for using flags in the Kondo and Lansing patents: because one of ordinary skill in the art would have recognized that use of identifying a state of a first flag and a state of a second flag in the data packet; and selectively verifying a checksum based on the state of the first flag and the state of the second flag would have provided a flexible arrangement whereby the packet creator can decide whether CRC is needed (Abstract in Lansing) and would have provided flagging for erroneous data for use by system controllers (col. 35, lines 55-62 in Kondo) and ould havew provided control information for checksumming (Abstract in Thompson).

However Maezawa, Kondo, Lansing and Thompson do not explicitly teach the specific use of a logical partitioned data processing system.

Hefferon, in an analogous art, teaches use of a logical partitioned data processing system (Abstract in Hefferon).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Maezawa, Kondo, Lansing and Thompson with the teachings of Hefferon and Bean by including use of a logical partitioned data processing system. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that use of a logical partitioned data processing system would have provided

highly efficient operation of a plurality of different programming systems in the different zones of the system (col. 1, lines 9-13 in Bean).

35 U.S.C. 103(a) rejection of claims 2, 16 and 30.

Col. 39, lines 55-67 in Kondo teaches a second ECC flag in a packet indicating whether errors are present in the packet or not. Step 905 in Figure 9 and claim 1 in Lansing teaches identifying a state of a first CRC flag used to indicate the presence of redundancy.

The Examiner asserts that a ECC flag indicates if there is an error when it is set is also an ECC flag that indicates that there is no error when the flag is not set, hence; an ECC flag indicates if there is an error is also a checksum good flag since it can indicate no errors when the flag is not set.

Thompson teaches responsive to receiving the data packet at a first partition of a data processing system from a second partition of a data processing system, identifying a state of a first flag and a state of a second flag in the data packet (Col. 3, lines 40-49 and col. 8, lines 13-27 of Thompson teaches checksum control information including first flag 74 and second flag 72, responsive to receiving the data packet at a first partition 22 in Figure 2 of Thompson of a data processing system from a second partition 12 in Figure 2 of Thompson of a data processing system, is used for identifying a state of first flag 74 and a state of second flag 72 in the data packet in order to verify datqa); and selectively verifying a checksum, by the first partition in the logical partitioned data processing system, for the data

packet as indicated by the state of the first flag and the state of the second flag (Col. 3, lines 40-49 and col. 8, lines 13-27 of Thompson), wherein the first flag and the second flag are both checksum-based flags that indicate checksum characteristics associated with the data packet (col. 8, lines 13-27 of Thompson).

35 U.S.C. 103(a) rejection of claims 3, 17 and 31.

Steps 905-915 in Figure 9 of Lansing teaches verifying the CRC, if CRC is present indicated by the first CRC flag and col. 39, lines 62-67 in Kondo teaches that verifying the checksum, if there are no errors in the packet indicated by the second ECC flag. Note: the flags in Kondo and Lansing are two distinct flags, the flag in Kondo providing an indication of whether redundancy exits (Note: ti is well known that some protocols such as UDP do not require redundancy whereas TCP does; in a multi-protocol system such as the one in Maezawa this information is critical since checksum verification can only take place if redundancy exists) and the flag in Lansing indicates whether an error has been detected in a network device such as the switching device 7 in Maezawa used to forward data to an intended receiver). Col. 39, lines 62-67 in Kondo explicitly teaches performing a CRC check (i.e., checksum verification) responsive to the ECC flag. CRC generation is responsive to the CRC flag in Lansing and since the CRC check (i.e., checksum verification) in both Kondo and Maezawa (and implicitly in Lansing) is **based on** the presence of CRC, the CRC check (i.e., checksum verification) is also **based on** the CRC flag.

35 U.S.C. 103(a) rejection of claims 4, 18 and 32.

Steps 905-915 in Figure 9 of Lansing teaches skipping the verification step, if no CRC is present indicated by the first CRC flag. Note: the flags in Kondo and Lansing are two distinct flags, the flag in Kondo providing an indication of whether redundancy exits (Note: ti is well known that some protocols such as UDP do not require redundancy whereas TCP does; in a multi-protocol system such as the one in Maezawa this information is critical since checksum verification can only take place if redundancy exists) and the flag in Lansing indicates whether an error has been detected in a network device such as the switching device 7 in Maezawa used to forward data to an intended receiver). Col. 39, lines 62-67 in Kondo explicitly teaches performing a CRC check (i.e., checksum verification) responsive to the ECC flag. CRC generation is responsive to the CRC flag in Lansing and since the CRC check (i.e., checksum verification) in both Kondo and Maezawa (and implicitly in Lansing) is **based on** the presence of CRC, the CRC check (i.e., checksum verification) is also **based on** the CRC flag.

The Examiner asserts that if a packet does not have a checksum it is impossible to perform checksumming on the packet. The intent in Lansing is clear.

35 U.S.C. 103(a) rejection of claims 5, 19 and 33.

Col. 39, lines 62-67 in Kondo teaches that skipping the checksum verification, if there are errors in the packet indicated by the second ECC flag.

Note: Step 905 in Figure 9 and claim 1 in Lansing teaches identifying a state of a first CRC flag used to indicate the presence of redundancy. The Examiner asserts that regardless of what the second flag is, if no CRC is included a CRC cannot be performed, that is the CRC check will be skipped if the first flag is unset and the second flag is set since the is no CRC.

35 U.S.C. 103(a) rejection of claims 6-10, 14, 20-24, 28 and 34-38.

Kondo and Lansing teach adaptive parameters (Steps 905-915 in Figure 9 of Lansing teaches a first CRC flag used to indicate the presence of redundancy; Col. 39, lines 62-67 in Kondo teaches a second ECC flag in a packet indicating whether errors are present) for allowing a sending station to notify a receiving station whether a transmitted packet has redundancy for use in verifying the packet based on a first CRC flag and whether the packet has errors so that receiving controller can imitate error handling based on a second ECC flag intended for use in the particular embodiments of claims 6-10, 14, 20-25, 28 and 34-38.

The Examiner disagrees and asserts that the flags in Kondo, Lansing and Thompson are adaptively provided at each receiving and transmitting node and are adaptively set or unset at each node as packets are transferred across a communication system.

35 U.S.C. 103(a) rejection of claims 11 and 25.

Page 3 of the Applicant's specification teaches that virtual adapters are used to send packets to each other in an interpartition virtual network. Multiplexer channel devices 3

and 10 in figure 1 of Maezawa are examples of virtual adapters used for interpartition communications (see Abstract in Maezawa).

The Examiner asserts Claims 1-14 are a method for processing data. "wherein the first virtual adapter is a software device driver that has no associated physical hardware" is a statement of intended use for the method and fails to set forth a positive limitation for a method for processing data.

35 U.S.C. 103(a) rejection of claims 12 and 26.

Maezawa teaches a first generating means for generating a new data packet for a target destination (interface driver 33 in Figure 2 of Maezawa); second generating means for generating the checksum for the new data packet if the new data packet is to be sent outside of the interpartition virtual network by a physical network adapter (external interface protocol control circuit 37 in Figure 2 of Maezawa); and sending means for sending the new data packet to the target destination (multiplex/distribution control circuit 36 in Figure 2 of Maezawa).

35 U.S.C. 103(a) rejection of claims 13 and 27.

Maezawa teaches means for sending the new data packet to the target destination using one of the physical network adapter (external interface protocol control circuit 37 in Figure 2 of Maezawa) or a virtual network adapter (link connection control circuit 38 in Figure 2 of Maezawa).

The Examiner asserts that col. 8 in Thompson explicitly teaches header control information that is added to a packet during preparation for transmission to inform a receiver appropriate actions to be taken upon receipt of the packet. Col. 8, lines 14-29 teach "Checksum control header is shown to include a start offset field 71, a stop offset field 75, an algo field 72, a direction field 73, an insert field 74 and an insert offset field 76" to selectively indicate to a receiver "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" "the direction of data flow (inbound or outbound)" and "whether the outbound packet is to have a checksum inserted" provided to inform a reception node whether checksumming is to be performed and, if checksumming is to be performed, "the byte at which checksumming is to start", "the number of bytes which are to be checksummed", "the checksum algorithm used (TCP, UDP, etc.)" and "the direction of data flow (inbound or outbound)". That is, the checksum control information is provided to inform a receiving node of critical information regarding CRC so that a receiving node can selectively control whether checksumming is to be performed and, if checksumming is to be performed, how it is to be performed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph D. Torres whose telephone number is (571) 272-3829. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Joseph D. Torres
Primary Examiner
Art Unit 2112

/Joseph D. Torres/
Primary Examiner, Art Unit 2112